CHAPTER

13

DEPLOYING WINDOWS 2000 USING REMOTE INSTALLATION SERVICES

After completing this chapter, you will be able to:

- Understand what RIS is and how it functions
- Understand the requirements for RIS
- Identify RIS client and server components
- Set up and configure RIS
- Create RIS images
- Create RIS boot disks
- Manage RIS security

In the previous three chapters, 10, 11, and 12, we have discussed components of Microsoft's IntelliMirror technologies, which provide a desktop management solution for Windows 2000 networks. In this chapter, we focus on the last component involved in a complete change and configuration management strategy: Remote Installation Services (RIS). With RIS, administrators are able to automate the installation of Windows 2000 Professional workstations over the network.

At this point, NT 4 administrators might be asking, "So what? Couldn't I do the same thing with answer files in NT 4?" The answer is an unequivocal "No!" Through answer files, an administrator could automate an NT 4 installation by including in the text file the appropriate responses to the questions with which a user would be prompted during installation—network settings, computer name, and so on. However, if you had no installation CD and you needed to install a custom image from the network, or if you didn't have a boot disk with DOS network card drivers, you were pretty much out of luck.

With RIS, if you have a compliant client computer, you can get network connectivity and choose from any number of administrator-created images with which to install and configure Windows 2000. With that in mind, let's look at an overview of what RIS does and how it functions.

RIS Overview

The simplest way to define RIS is as follows: RIS is a Windows 2000 Server component that allows Windows 2000 Professional to be installed remotely onto a system without a support technician needing to actually touch the computer. Combined with the other IntelliMirror technologies we have previously discussed—such as data management (folder redirection, offline folders), desktop settings management (roaming profiles and Group Policy settings that follow a user, group, or computer), and software installation and management—RIS completes a total desktop management solution. Through these technologies included in Windows 2000, an administrator can effectively deploy new PCs and even reinstall existing PCs from a central location, without having to visit a user's office. This ability is a tremendous time saver for IT departments; it frees staff members from less productive work (reinstalling/repairing software) so that their talents can be used more efficiently elsewhere.

In addition, with IntelliMirror, users no longer have to sit and wait unproductively for an IT staff member to show up after they have placed a call to the help desk. With RIS, even the entire operating system (OS) can be reinstalled upon request: A preconfigured OS image can be applied to the computer, and the user needs to supply only logon information.

Before we get into the details of how RIS works, it is extremely important to note that the process of applying an OS image to a computer through RIS *erases all existing data on the hard drive*. For obvious reasons, it is important to ensure that any nonreplaceable user information is backed up prior to reinstalling the OS. Because RIS erases the hard drive, it cannot be used to upgrade an existing OS, such as Windows 98 or NT Workstation 4. Furthermore, RIS can be used to install only Windows 2000 Professional—you cannot install Windows 9*x* or NT with RIS. To automate an OS upgrade or install a non–Windows 2000 Professional OS on a client PC, you need to look at a full-blown systems management utility such as Microsoft Systems Management Server (SMS).

To realize the power of RIS and IntelliMirror fully, imagine a situation where the hard drive in a user's compliant PC has had a hardware failure. A desktop support technician must go to the user's office and replace the hard drive with a new one. So far, nothing out of the ordinary has happened. However, instead of having to sit there half a day reinstalling the OS and all the applications, the technician can activate an RIS installation and walk away. The user only needs to type in a username and password, and the rest of the process of installing Windows 2000 Professional proceeds automatically.

Once the OS is installed, the user logs on to the network. Group Policy runs, and through Software Installation and Maintenance settings (assigned and published applications) and desktop settings management, the user has access to all their applications and their desktop. Start menu settings return to the state they were in prior to the hard-drive crash. The user can begin productive work immediately—and all of this takes place automatically, without any intervention by an administrator or desktop support technician.

How RIS Functions

RIS works by creating a Pre-Boot Execution Environment (PXE), which enables a compliant client PC to gain basic TCP/IP network connectivity. PXE (pronounced "pixie") technology is not integrated into every network card, so you must ensure that you have a PXE-compliant adapter before you can use RIS. The client requirements for RIS are listed in the next section.

Once network connectivity is established, a series of scripts can be run to bring the client to the point of installing the OS. For NT 4 administrators, this ability makes RIS a must-have item. In the past, administrators often experienced the frustration of trying to reinstall an OS on a computer without a boot floppy or installation CD handy. You knew all the software you needed was on the network, and the computer on which you were trying to reinstall the OS had a network card, but you couldn't get network connectivity established. RIS ends that frustration, because network connectivity is established at the hardware level through the interaction of the network card with the network. The details of this interaction will be discussed later in the chapter.

With RIS, an administrator can choose to have a computer go through a CD-like installation of Windows 2000 Professional, as if a normal installation is taking place from a CD. Alternatively, you can customize the installation to the point of scripting it with an answer file, so that the user is not required to choose any options during setup.

Now that you have a basic understanding what RIS does, let's discuss the components required for RIS.

RIS Requirements

In order for RIS to function, a number of components must already be installed and configured on a Windows 2000 network. They are:

- Remote Installation Services
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP) Server
- Active Directory

In the next sections, we will discuss each of these Windows 2000 components as they relate to using RIS.

Remote Installation Services

Windows 2000 includes RIS as an optional component that can be installed through the Windows Components Wizard of the Add/Remove Programs applet in Control Panel. RIS runs as a service on at least one Windows 2000 Server system on the

network, listening for client requests. In addition, the RIS server stores the OS images that the client computer can choose from when it invokes RIS. You can use Group Policy to determine which images should be available to which users.

Setting up an RIS server is discussed later in this chapter.

Domain Name System (DNS)

DNS is the service that enables RIS clients to find RIS servers on the network. Windows 2000 RIS servers register themselves in DNS, so that when an RIS client establishes network connectivity, it has the name and Internet Protocol (IP) address of an RIS server from which to pull an image. Microsoft DNS is not required as long as the third-party DNS server you use supports Requests for Comments (RFCs) 2052 (SRV RR) and 2136 (dynamic updates).

Dynamic Host Configuration Protocol (DHCP) Server

In order to establish network connectivity, an RIS client must have an IP address. Because the process all takes place at the hardware level, there is nowhere to assign a static IP address. RIS therefore uses dynamic addressing in order to obtain an IP address and connect to the network. For an RIS client to obtain a dynamic address, a DHCP server must be running on the network. It can be either a Microsoft DHCP server or a third-party DHCP server.

Active Directory

RIS is dependent on Active Directory in order to function. The reason is twofold. First, RIS uses Group Policy, which is dependent on Active Directory, in order to determine permissions for user accounts and computer accounts prior to supplying RIS image choices to the user. Second, RIS uses network configuration settings stored in Active Directory to determine information such as which RIS server should be used in the case where multiple RIS servers exist on a network. In addition, Active Directory information is used for such things as implementing a standard naming convention for new computers and determining in which domain or Organizational Unit to place the new computers.

With an understanding of RIS's dependencies, let's look at the server and client components that make up RIS.

RIS Client and Server Components

In addition to the RIS dependencies we just listed, components at both the client and server enable RIS to function. In this section, we will discuss the client and server components of RIS.

Client Requirements of RIS

A client computer must meet a number of requirements in order to use RIS. These requirements are:

- Computer must meet NetPC or PC98 standards
- Computer must have a compliant BIOS
- Computer must have a compatible network adapter

NetPC or PC98 Standards

A computer can meet the requirements of RIS by conforming to the NetPC or PC98 standard. A client computer that meets the requirements set forth by either the NetPC or PC98 standard will include PXE functionality. Compliant computers must have version 1.0b at minimum to work with RIS.

Additional standards exist within the NetPC and PC98 standards, but for the purpose of this book only PXE and Plug and Play requirements are discussed.

Compliant BIOS

A PC can also meet the requirements of RIS by having a compliant motherboard BIOS, which will include the necessary PXE functionality for RIS. If you don't currently have a PXE-capable motherboard, see the manufacturer about a possible flash upgrade (almost all motherboards are now upgradeable).

Compatible Network Adapters

In addition, a compliant client computer can simply have a compatible network adapter installed in order to use RIS. A compliant network adapter will be PXE compliant, meaning it supports the preboot execution environment standard. Due to Plug and Play requirements, a compliant network card will also be PCI based. This excludes Personal Computer Memory Card International Association (PCMCIA) network adapters typically found in laptops; so, if you want to use RIS with a laptop system, you must first connect the laptop to a docking station containing a Peripheral Component Interconnect (PCI) network adapter that also has PXE functionality.

If the motherboard is not compliant and the computer does not meet NetPC or PC98 standards, and you don't have a PXE-compliant network adapter, it might still be possible to still use RIS. Windows 2000 includes an RBFG.EXE utility that allows an administrator to create a bootable floppy disk that emulates the PXE environment. Creating boot floppies for RIS is discussed in detail later in this chapter.

Windows 2000 doesn't support a large number of non-PXE-compliant network cards, but Table 13-1 lists them.

Table 13-1 Compatible network adapters supported by the RIS boot floppy

Manufacturer	Model
3Com	3C900B-Combo 3C900B-FL 3C900B-TPC 3C900B-TPO 3C900-Combo 3C900-TPO 3C905B-Combo 3C905B-FX 3C905B-TX 3C905C-TX 3C905-T4 3C905-TX
AMD	AMD PCnet Adapters
Compaq	NetFlex 100 NetFlex 110 NetFlex 3
DEC	DE450 DE500
HP	Deskdirect 10/100 TX
Intel	Pro 10+ Pro 100+ Pro 100B
SMC	8432 9332 9432

Hardware Requirements

In order to use RIS on a client computer, the client must meet the following hardware requirements:

- Pentium 166 or faster CPU
- 32MB of RAM minimum (64MB recommended)
- 800MB or larger hard drive
- DHCP PXE-based boot ROM or network adapter supported by the RIS boot floppy

Client Installation Wizard

The Client Installation Wizard is the client-side piece for RIS, which is downloaded to the client and communicates with the RIS server. A default set of screens is presented to the user; these screens are provided by the Boot Information Negotiation Layer

(BINL) server-side service. They guide the user through the Client Installation Wizard to log on and select Windows 2000 Professional installation options that have been defined by the administrator. The user invokes the Client Installation Wizard by pressing F12 once the PC's power-on self-test (POST) process has completed and before the OS starts booting.

It is important to note that the boot process is not secure: Information is sent over the network in clear text that can be read with a packet sniffer. Therefore, you should ensure that only limited RIS servers are on the network, and that you have control over who is allowed to set up and configure RIS servers in general.

Now, let's look at the server components for RIS.

Server Components of RIS

The RIS services on a server are less dependent on specific hardware than are client computers, although you must make note of some hardware requirements. These requirements are:

- Pentium 166 or faster CPU (200+ recommended).
- 96 to 128MB of RAM required when running Active Directory, DNS, and DHCP services.
- 10MB Ethernet adapter (100MB recommended).
- Access to Windows 2000 Professional installation files (can be CD-ROM, network share, or local directory with a copy of the files).
- 2GB hard-disk space for the RIS servers folder tree. It is recommended that you devote an entire hard-disk partition to the directory tree for RIS.
- NTFS-formatted partition for RIS images. RIS cannot be installed on Distributed File System (Dfs) or Encrypted File System (EFS) volumes.

As we previously discussed, the requirements to use RIS from the server end include Active Directory, DNS, DHCP, and the Remote Installation Services service. When RIS is installed through Add/Remove Programs (RISetup.exe is the program that actually installs RIS, as discussed later), additional services are installed on the server. These services include:

- *Boot Information Negotiation Layer (BINL)*—As discussed previously, this service listens for client DHCP/PXE requests. In addition, BINL redirects clients to the appropriate files needed for installation during the Client Installation Wizard. The BINL service also verifies logon credentials with Active Directory.

- *Trivial File Transfer Protocol Daemon (TFTPD)*—RIS uses TFTP to initially download to a client all files necessary to begin the Windows 2000 Professional installation. Included in this download is Startrom.com, which is the bootstrap program that displays the message for the user to press F12 for Network Service. If the user does press F12 within three seconds, the Client Installation Wizard is downloaded through TFTP to the client computer.
- *Single Instance Store (SIS)*—The SIS service seeks to reduce disk space requirements for RIS images by combining duplicate files. The service contains an NTFS file system filter (RIS, as you will recall, can be installed only on an NTFS partition) and the service that manages images on the RIS installation partition.

Another server component, RIPrep.exe, is used to create RIS images. Creating RIS images is discussed later in this chapter.

Now that we have discussed the basics of RIS, let's get our hands dirty with an RIS installation.

Setting Up and Configuring RIS

If you perform a typical installation of Windows 2000 Server at the time you run Setup, RIS is not installed. RIS is an optional component that can either be selected in a custom setup or added later through the Windows Components Wizard of the Add/Remove Programs applet in Control Panel. When you launch the Windows Components Wizard, as shown in Figure 13-1, you have a choice of components that you can add or remove. Put a check mark in the box for Remote Installation Services and click on Next.

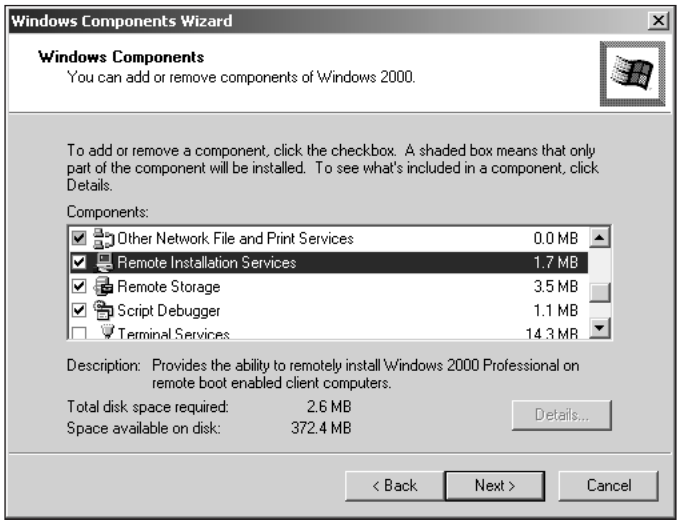

Figure 13-1 The Windows Components Wizard

Once you click on Next, the installation wizard begins configuring RIS, as shown in Figure 13-2. Windows 2000 installs RIS services, but it does not actually allow any configuration of RIS during this initial setup. After RIS is installed, you will see the window shown in Figure 13-3. Click on Finish, and restart your computer when prompted.

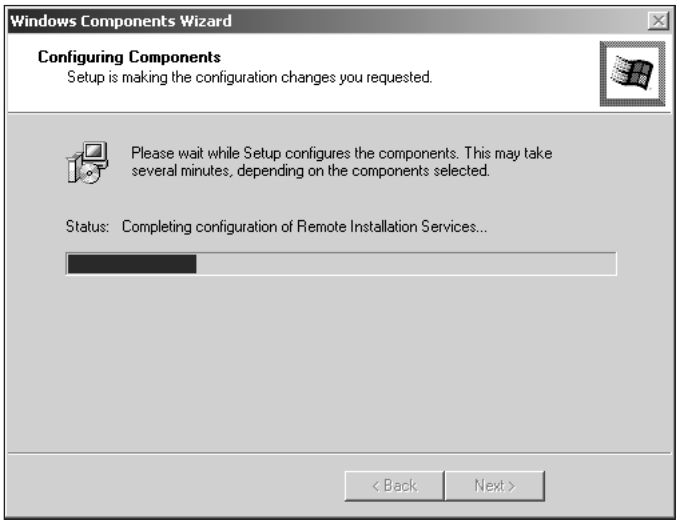

Figure 13-2 Windows 2000 installs the RIS service to the hard drive, updating the system in the process

Figure 13-3 After RIS is installed, click on Finish and then restart the computer

RISetup

Once RIS is installed and you have restarted your computer, it is still necessary to configure RIS. RISetup.exe is the utility used to configure RIS, and you can invoke it from the Run line. The Remote Installation Services Setup Wizard, shown in Figure 13-4, prepares the server to be an RIS server. In the following sections, we will walk through the setup and configuration of an RIS server.

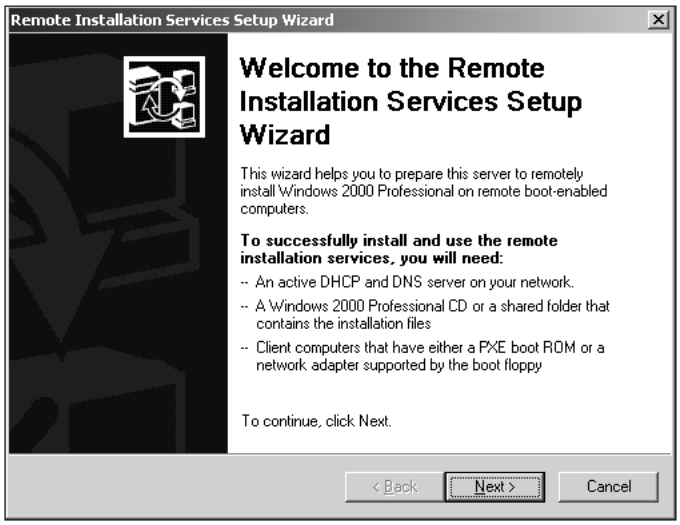

Figure 13-4 The Remote Installation Services Setup Wizard is invoked through the RISetup.exe command

The first option you are presented with, shown in Figure 13-5, is the installation directory for RIS. Note that this directory must reside on an NTFS partition with sufficient disk space for your RIS images. If you attempt to install to a non-NTFS partition, the Setup Wizard will give an error message. Windows 2000 will provide a default drive and directory, but the drive may or may not be valid (the wizard does not check the drive for file system type and disk space before offering it as a choice). Therefore, you may have to choose a different drive for your RIS installation. In most cases, however, you should leave the default directory name.

The next step in your installation is to decide whether your RIS server will immediately begin servicing requests once you have completed Setup, as shown in Figure 13-6. By default, RIS services do not begin immediately after Setup. This is primarily a security measure. Because you really can't use RIS anyway, until you've created an RIS image, there is little sense in having the services running when—as we mentioned earlier—

RIS data is sent to and from the server in clear text. An unscrupulous individual could exploit your new RIS server if it were online before you were ready to start using it. In most environments, though, enabling RIS probably isn't much of a security risk.

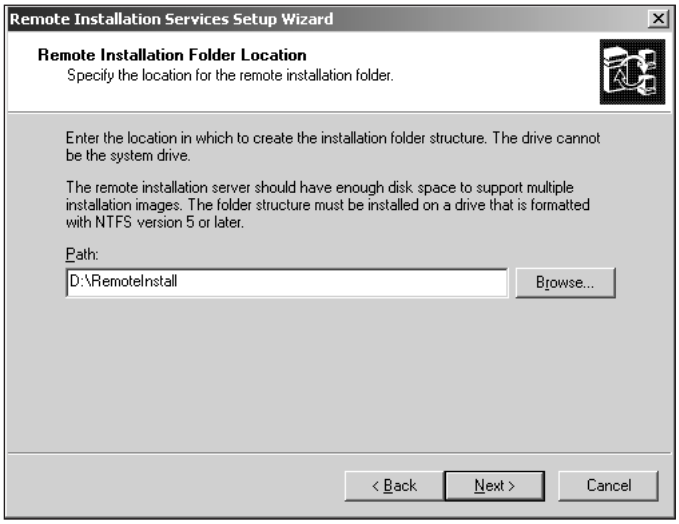

Figure 13-5 The first step in installing RIS is to choose an installation directory

Figure 13-6 You can choose whether to start servicing RIS clients immediately, and whether RIS should respond to unknown computers

In addition to deciding whether to start RIS, you can choose whether RIS should respond to unknown computers. Select your choices, and then click on Next.

The next step in configuring RIS is to point Setup to the installation files for Windows 2000 Professional, as shown in Figure 13-7. This location can be a CD or a network path, as in our example. Once you have defined your directory, click on Next.

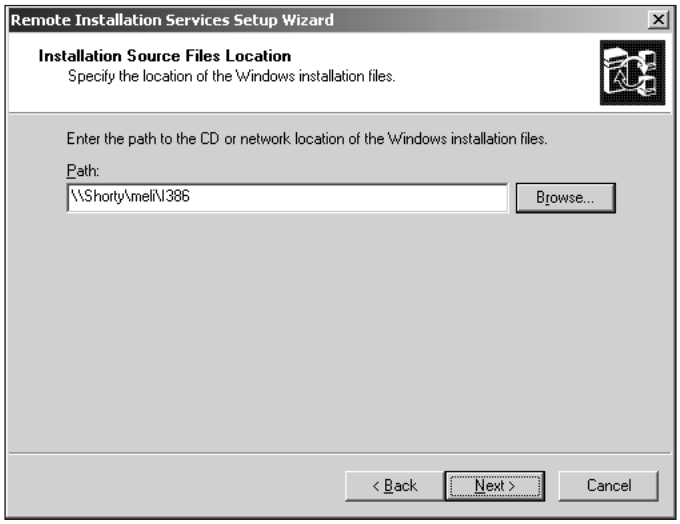

Figure 13-7 You can define the installation directory for Windows 2000 Professional as either a CD or a network path

Now, the Setup Wizard prompts you for the name of the folder to copy the Windows 2000 Professional setup files to on the RIS server. Unless you have a specific need to change it, the default directory supplied by RIS Setup, illustrated in Figure 13-8, should be fine.

The next step is to determine a friendly description for your RIS image, and the help text that will be shown in the Client Installation Wizard when the user presses F12 to start RIS on the client. Figure 13-9 shows an example.

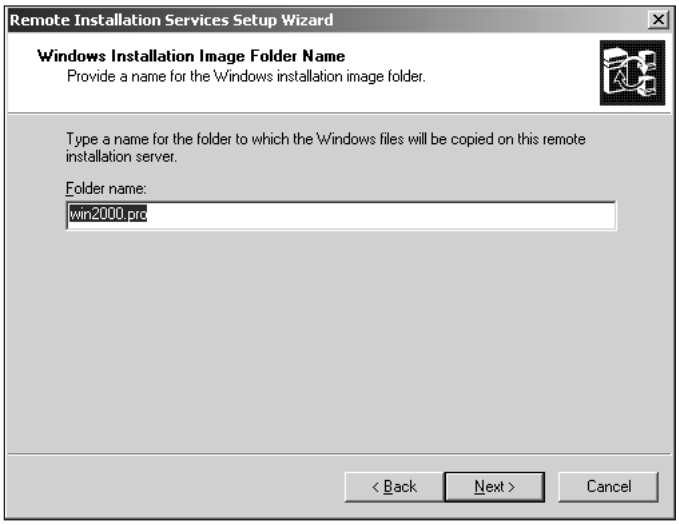

Figure 13-8 RIS Setup next offers a default directory to copy the Windows 2000 Professional setup files into on the RIS server

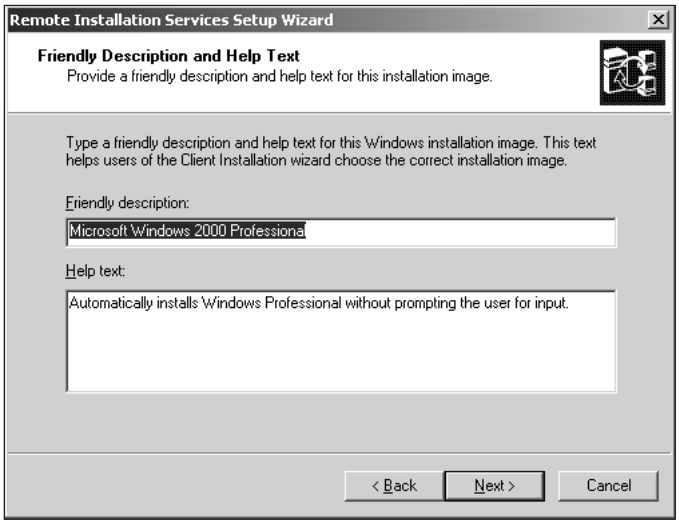

Figure 13-9 Assigning a friendly description to the RIS image makes it easier to determine what RIS image to use when choices are presented in the Client Installation Wizard

Before Setup actually begins, you are given the chance to review your settings and go back to change any settings. Once you click on Finish, as shown in Figure 13-10, installation begins. Figure 13-11 shows RIS Setup as it runs through its task list.

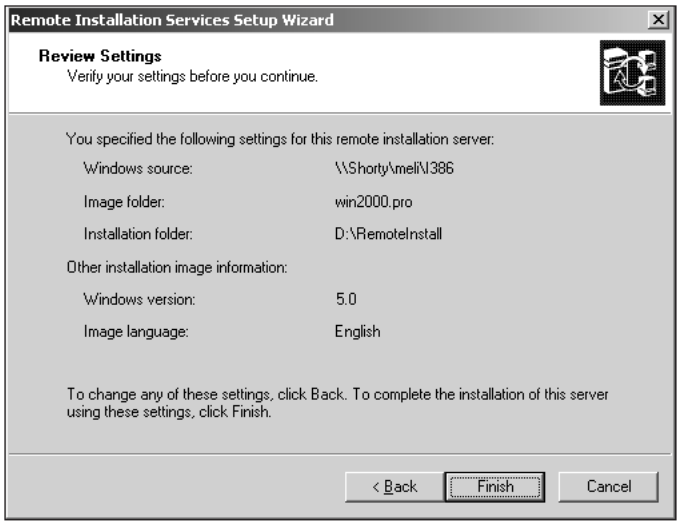

Figure 13-10 You have a chance to review your installation options before proceeding with the actual installation

After you have configured RIS, you can go into Windows Explorer and look at the new directory structure. It will look something like that shown in Figure 13-12 if you didn't make any changes from the defaults.

Figure 13-11 The Remote Installation Services Setup Wizard completes the list of tasks as it configures RIS

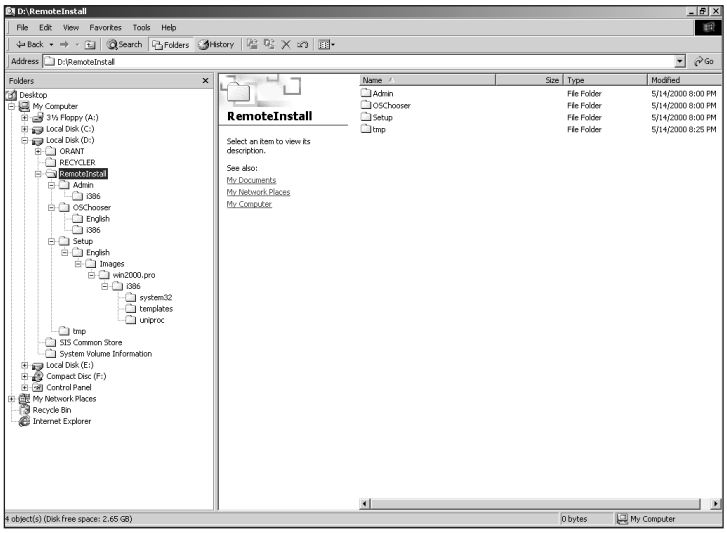

Figure 13-12 RIS Setup creates this directory structure during the Setup Wizard

Now that we have set up and configured RIS, let's look at creating additional RIS images and creating RIS boot disks.

Creating RIS Images

As we have seen, CD-based RIS images can be created through the RISetup utility. Additionally, the RIPrep.exe utility allows you to clone a standard corporate desktop for deployment to other systems. In this section, we will examine the RIPrep utility and also learn about creating RIS boot disks for compatible network adapters.

RIPrep

Unlike RISetup, which allows only an administrator to deploy a CD-based setup of Windows 2000 Professional (even a network-based installation is just a copy of the files from the CD shared on a network drive), RIPrep can be used to deploy the OS plus customized settings and even locally installed desktop applications. This process is not the true disk cloning that products like Norton Ghost provide, because it can be used only with Windows 2000 Professional. In addition, RIPrep does not support multiple hard drives or multiple partitions on the computer where the image is being created.

Other limitations of RIPrep include the requirement that a CD-based image with the same version and language as the RIPrep image also exist on the RIS server, and that the

target system must have the same hardware abstraction layer (HAL) as the system used to create the image. By having the same HAL, an image created on a single processor system cannot be installed onto a dual-processor system. Because Windows 2000 does not support Alpha processors like NT 4 does, you won't have to worry about mixing up Intel (I386) and Alpha images.

Although RIPrep has limitations, it offers advantages over using RISetup to create images. Most notably, RIPrep allows an administrator to create a standard desktop image and then use RIS to deploy it to new computers as they come in from an original equipment manufacturer (OEM). In addition, reinstallation of the OS is much faster from an RIPrep image, because the image is applied as a copy operation to the target hard drive and not run though an actual Windows 2000 installation, as would happen with a CD- or network-based RISetup image.

Creating Images with RIPrep

Creating an image with RIPrep is a two-step process:

1. Install and configure a computer with Windows 2000 Professional and the specific applications and settings you want to include in the image.
2. Run RIPrep.exe from the RIS server.

You must keep clear an important distinction: The RIPrep.exe utility is located on the RIS server, but it is *executed* from the RIS client on which the image is being created. From the client, choose Start|Run and type

```
\\RISserver\reminst\admin\i386\riprep.exe
```

If you attempt to run RIPrep.exe from a non-Windows 2000 Professional system, you will receive an error message stating that the utility will run only on Windows 2000 Professional. When you run RIPrep from a valid system, however, the Remote Installation Preparation Wizard starts, as shown in Figure 13-13.

Even though you ran RIPrep.exe from one RIS server, you do not necessarily have to copy the image you are creating to that particular server. Figure 13-14 shows the next step in creating an image with RIPrep, where you choose the RIS server to which to copy the image.

Figure 13-13 The Remote Installation Preparation Wizard is started by executing RIPrep.exe from a Windows 2000 Professional client computer

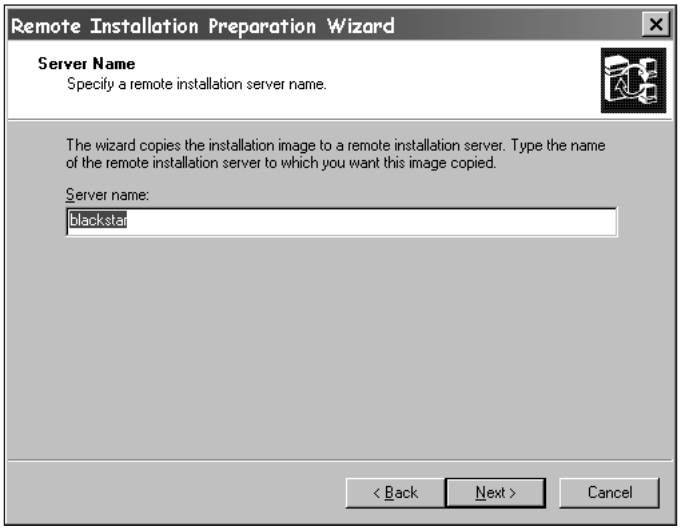

Figure 13-14 If you have multiple RIS servers on your network, you can choose which server should receive the image

The next step in creating the RIS image is to supply the name of the installation directory on the RIS server previously chosen. Typically, you would type the name of an existing directory only if you were replacing an existing image. If this new image will not be replacing an existing image, type in a new directory name as shown in Figure 13-15 and click on Next.

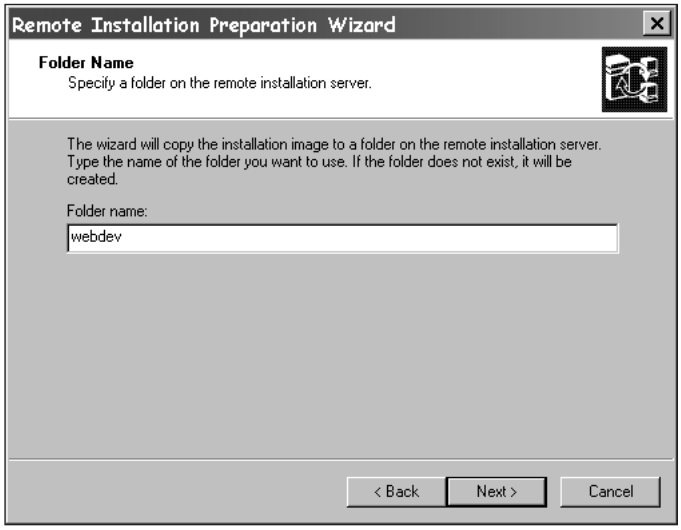

Figure 13-15 Supply a directory name on the RIS server for the Remote Installation Preparation Wizard to copy the image

In our example, the image is being created for a corporate Web developer environment. For that reason, we gave the directory the descriptive name *webdev*, in order to identify the image it contains on the RIS server.

In Figure 13-16, you can see the next step in creating an image, which is assigning a friendly name to the image and creating the help text. The friendly name displays in the list of available images during the Client Installation Wizard. The help text provides an additional description to help the user identify the correct image to use when acting as an RIS client. In our example (an RIS image for a Web development system), we list the applications that will be installed on the system along with the Windows 2000 Professional OS as part of the imaging process.

If you have any programs or services running that could interfere with the imaging process, Windows 2000 will warn you. Figure 13-17 lists a number of programs and services that were running on the RIS image source workstation at the time we created this example image. Once you have closed the programs and stopped the necessary services, click on Next.

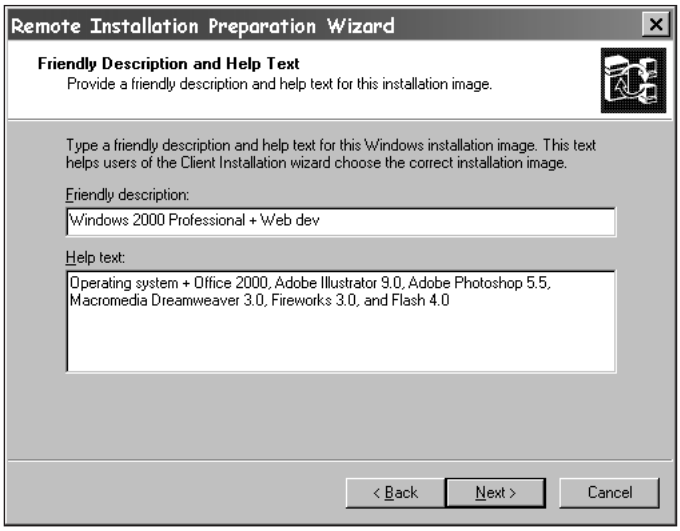

Figure 13-16 By assigning a friendly name and help text, users can identify the correct image to use during the Client Installation Wizard

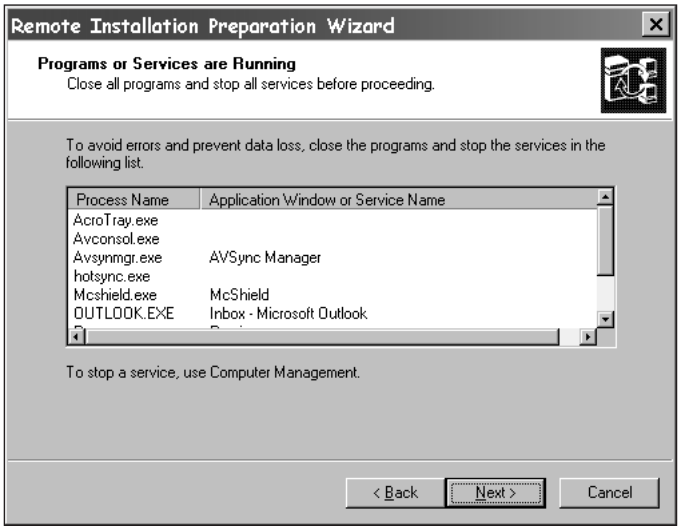

Figure 13-17 The Remote Installation Preparation Wizard prompts you to close any programs and services that might interfere with the imaging process

Before beginning the actual image creation, the wizard allows you to review your choices. Notice in Figure 13-18 that the folder name is incorrect. Initially, we created a generic folder that we intended to use for RIS images, only to decide later to create separate subfolders for each image. By reviewing the settings we had configured, we were able to back up through the wizard and change the folder name from *RISimages* to *webdev* before starting the actual image creation.

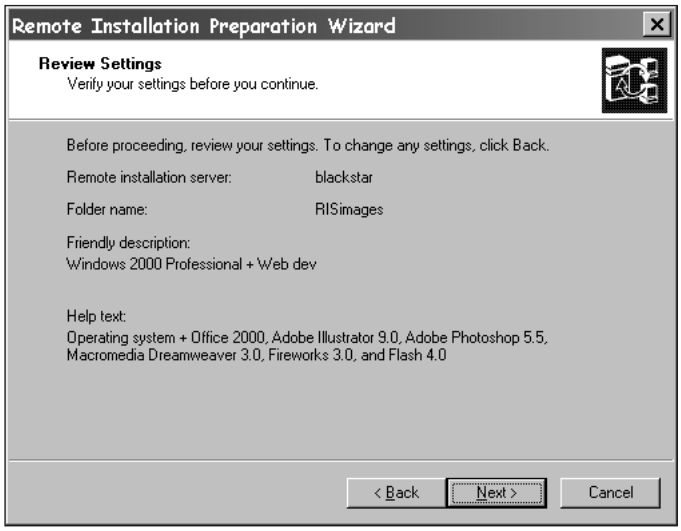

Figure 13-18 Before starting the actual image creation, take a moment to review your settings and ensure they are correct

The last step, shown in Figure 13-19, is an information dialog box from the Remote Installation Preparation Wizard that describes the process that is about to occur. Once you understand what is about to happen on your system, click on Next to continue. You can watch the RIPrep wizard image process taking place, as shown in Figure 13-20.

Figure 13-19 The RIPrep wizard informs you of how the image process will take place on your system before beginning

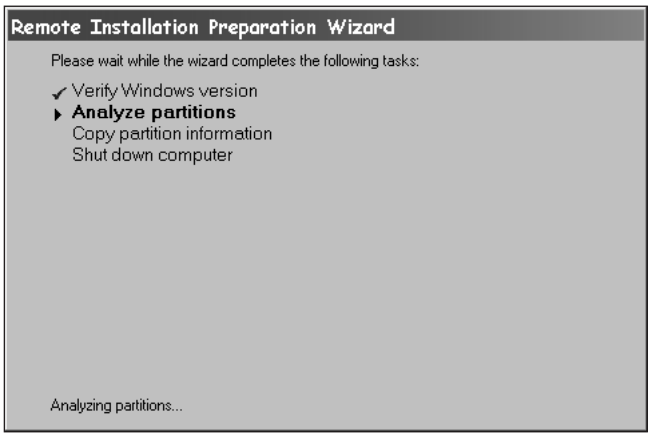

Figure 13-20 The RIPrep wizard displays the current status of the image process, showing the completed, current, and pending tasks

Images created by the RIPrep wizard are stored in the same subfolder as images created during RISetup. If you used the default settings when we examined the RISetup wizard earlier in this chapter, and you are using an English language version of Windows 2000 Server, your RIS directory structure will be as follows:

- *\RemoteInstall\Setup\English\Images\win2000.pro\i386*—The default image created during the RISetup wizard earlier. Subdirectories exist under i386 for this CD-based installation image for system32, templates, and uniproc.
- *\RemoteInstall\Setup\English\Images\webdev\i386*—The image directory we just created for our webdev image. A directory called Mirror1, which appears under i386, does not appear in the subdirectories of an RISetup-created image.

13

RIPrep Files

In addition to the directory structure created, you need to know what files are important to the RIPrep image. These files are as follows:

- *RIPrep.log*—This ASCII text file documents the Remote Installation Preparation Wizard image process, listing any errors and relevant information that might be of troubleshooting use to an administrator.
- *Bootcode.dat*—This file is located in the \Mirror1 subdirectory of the image's i386 folder. It contains the boot sector information for the client system.
- *Imirror.dat*—This file also is located in the \Mirror1 directory, and contains installation information about the image source computer, such as the installation directory and the HAL type.

It is worth repeating here that RIPrep can create images only for single-partition systems. If you have Windows 2000 Professional installed to a partition other than the boot partition, the RIS image process will fail.

Creating RIS Boot Disks

Creating an RIS boot disk is necessary if you do not have a PXE-capable network adapter or motherboard, but you do have a network adapter that is supported by the RIS boot disk creation utility, RBFG.exe. We briefly touched on the Windows 2000 Remote Boot Disk Generator previously, but we did not discuss creating disks. In this section, you will actually create an RIS boot disk.

There is not much to the Remote Boot Disk Generator. Essentially, as you can see from Figure 13-21, you have the option to view the supported adapter list or create the disk. The About page contains program credits; and if you have multiple floppy drives (does anyone still have two floppy drives?), you can choose which one to use to create the disk. The RBFG utility will erase the floppy in the drive without warning you first, so ensure that you select the right disk and drive before continuing.

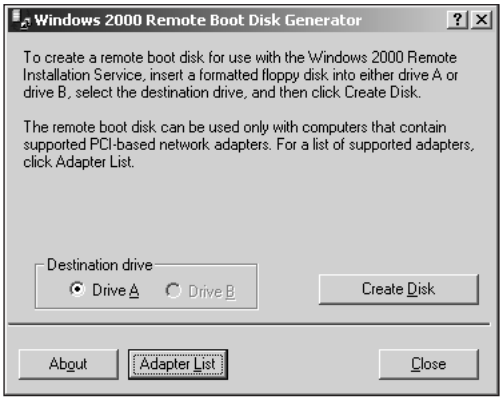

Figure 13-21 The Remote Boot Disk Generator allows you to create a network-bootable diskette for supported network adapters

Table 13-1, shown earlier, listed the supported adapters. To see the list on screen, click on the Adapter List button in the utility. The RIS boot disk emulates a PXE environment for these supported non-PXE-capable network adapters, and if you look, you will notice that the boot disk once created contains only a single file: RISDISK.

RISDISK has no file extension, and the file is only 90K in size. If you have a supported network adapter, however, this disk is all you will need to start the Client Installation Wizard.

Managing RIS Security

Security is always an important issue when discussing computer networking topics, and this is no different with RIS. As you've been reading about how RIS functions on a network, you might have been asking yourself what steps you could take as a Windows 2000 systems administrator in order to prevent unauthorized individuals from setting RIS servers, creating images, or even gaining network connectivity through RIS and installing an image. Fortunately, RIS has some built-in safeguards that will allow you to maintain some control over who is able to use Remote Installation Services. Some of these security services include requiring RIS servers to be authorized before they can respond to RIS client requests, being able to use Group Policy to manage RIS client installation options, and editing configuration settings through the Active Directory Users and Computers administrative tool.

Authorizing an RIS Server

Before an RIS server can service client requests, it must first be authorized into Active Directory. Authorization can be done a few different ways. First, during the Remote Installation Services Setup Wizard, you can choose to have the RIS server start responding to client requests immediately upon completion of the wizard. This is not the recommended method of authorization, and, by default, the box to enable immediate authorization is not checked.

Second, if you install RIS onto a server that is not already an authorized DHCP server, you can authorize RIS through the DHCP administrator tool. In the DHCP Microsoft Management Console (MMC), right-click on the DHCP root node of the tree and select Manage Authorized Servers. Click on the Authorize button and type in the fully qualified domain name (FQDN) or IP address of the RIS server. Confirm that this is the server you want to authorize, and you are set.

You might wonder why you would need to use the DHCP MMC console to authorize an RIS server. Windows 2000 requires DHCP servers to be authorized in Active Directory as well before they can begin distributing IP addresses to clients, similar to the requirements for RIS. Because RIS is dependent on DHCP, it makes sense to use a similar authentication scheme for bringing new RIS servers into an Active Directory network. That said, we find the last method of authorization ties in with DHCP.

The last method is the easiest. If you install RIS onto an authorized DHCP server, you do not have to take any further steps to authorize RIS. The authorization will be passed along from DHCP to RIS because the server is already authorized in Active Directory.

In order to authorize an RIS server, the account you are logged on with must be a member of the Enterprise Admins security group.

Troubleshooting RIS Authorization

If you are having trouble getting an authorized RIS server to respond to client requests, it might be because the changes haven't yet taken effect in Active Directory. You can speed up the process, though, by opening a command prompt and typing the following:

```
secedit /refreshpolicy /MACHINE_POLICY
```

You might remember that command from our discussion of Group Policy implementation in Chapter 10, where we needed to make Group Policy settings we had changed take effect immediately.

Managing RIS Client Options with Group Policy

For an additional measure of security, Windows 2000 enables the administrator to configure options that define the behavior of the Client Installation Wizard. Specifically, the options that can be configured are the choice options presented to users when they invoke RIS through F12.

The choice options are configured through the Remote Installation Services node of the User Configuration container in the Group Policy Editor. Because this is Group Policy, you can apply these settings at the site, domain, or Organizational Unit (OU) level. You might want to use the Default Domain Policy, or you might want to configure different policy options for different OUs. No matter where you choose to apply the policy, you edit it the same way. Open the Group Policy Editor and navigate to the Remote Installation Services node, as described earlier. In the pane on the right side of the editor, right-click on Choice Options and click on Properties. You will see a dialog box like that in Figure 13-22, which shows the following client options:

- *Automatic Setup*—Set to Don't Care by default, which means it inherits its settings from the parent container. Eventually, through inheritance, this policy will be defined as Allow or Deny.
- *Custom Setup*—Denied by default. Allows users to install custom RIPrep-created images.
- *Restart Setup*— Denied by default. Determines if a setup that failed to complete for whatever reason will be allowed to be restarted.
- *Tools*—Denied by default. Allows access to maintenance and troubleshooting tools such as disk utilities and antivirus software. An administrator might make these types of tools available for troubleshooting purposes.

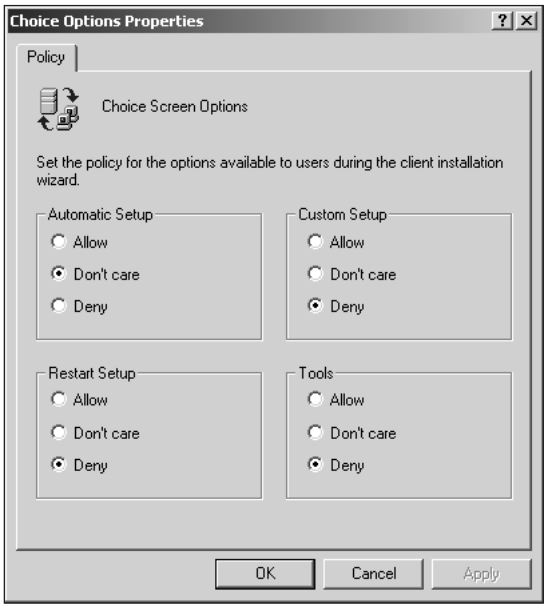

Figure 13-22 An administrator can configure client choice options for additional RIS security

Managing RIS Configuration Settings

The strongest security settings you can configure for RIS lie within the Active Directory Users and Computers administrative tool. Through this utility, you can perform the following tasks as they relate to RIS:

- Configure client support
- Define a computer naming convention
- Grant computer account creation rights
- Prestage computers

Configuring Client Support

In order to configure client support, which includes whether RIS should respond to clients and whether the RIS server should respond to unknown computers, open Active Directory Users and Computers. Next, open either the Domain Controllers or Computers folder (depends on the type of server on which you installed RIS), right-click on your RIS server, and choose Properties. Click on the Remote Install tab, which will bring up a property sheet like that in Figure 13-23.

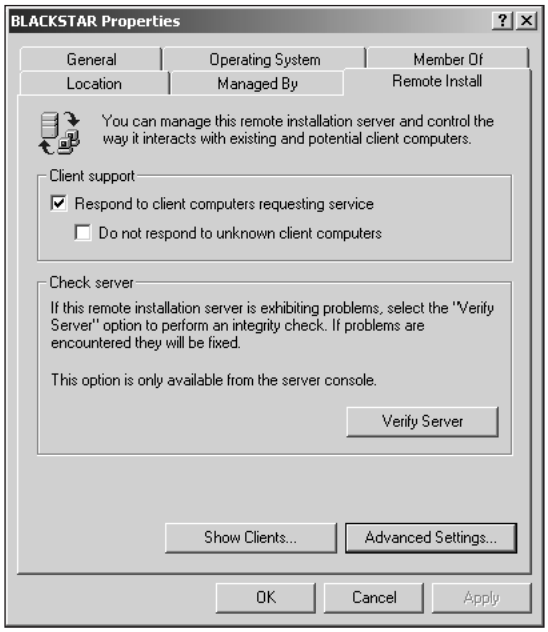

Figure 13-23 The Remote Install property sheet contains RIS server configuration settings

Defining a Computer Naming Convention

In addition to configuring the client support, you can choose Show Clients to search the Active Directory for known RIS client computers. For more security settings, however, click on the Advanced Settings button, which brings up the property sheet shown in Figure 13-24. Through this property sheet, you can define a computer naming convention for RIS clients. In most cases, you will not want users to come up with their own computer names when installing Windows 2000 Professional. If they do, you'll end up with a network full of nonstandard names that make administrative life difficult. Through Advanced Settings, you can determine not only what the naming convention will be, but also where in Active Directory the computer account will be created.

Note that if you choose a naming convention and an Active Directory location for the computer accounts, the user account under which the Client Installation Wizard is run must have the necessary permissions to add computer accounts to the domain.

Granting Computer Account Creation Rights

In order to be able to use the Client Installation Wizard to install Windows 2000 Professional into a domain, a user needs to have Read permission to the OU that has been defined as the Active Directory location for the new computer account. The user also must have permissions to create Computer objects.

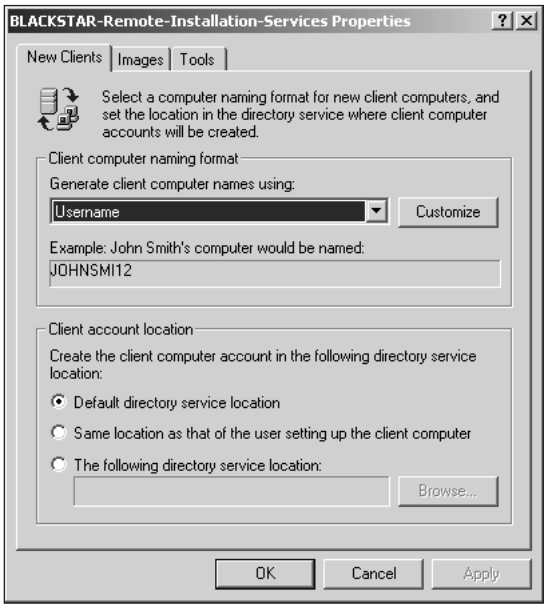

Figure 13-24 The Advanced Settings property sheet contains additional settings to tighten RIS security

In order to ensure a user has Read permission to the required OU, first click on View and select Advanced Features if it is not already selected in Active Directory Users and Computers. Next, right-click on the desired OU (such as Computers) and choose Properties. Then, click on the Security tab. Highlight Authenticated Users and verify that a check appears in the Read box under the Allow column, at minimum.

To allow a user permission to create Computer objects, you will need to use the Delegation Of Control Wizard. Right-click on the OU that will hold the computer account and choose Delegate Control. Select a group or user and click on Next. You will see a dialog box like that in Figure 13-25. Rather than delegate control of everything in this folder, which are far too many permissions for the simple task the user needs to complete (adding their computer account), choose the Only The Following Objects In The Folder option. Select Computer Objects from the list and click on Next. Choose Read and Write permissions, which will automatically select related permissions throughout the list, as in Figure 13-26.

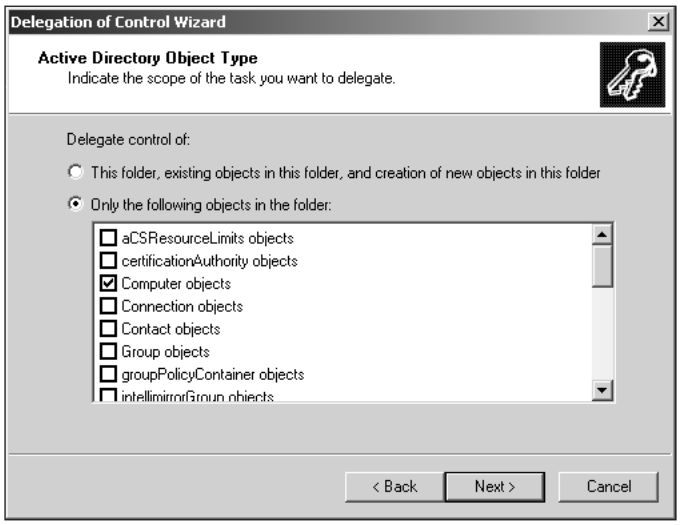

Figure 13-25 The Delegation of Control Wizard allows you to delegate Computer object creation to other users and groups

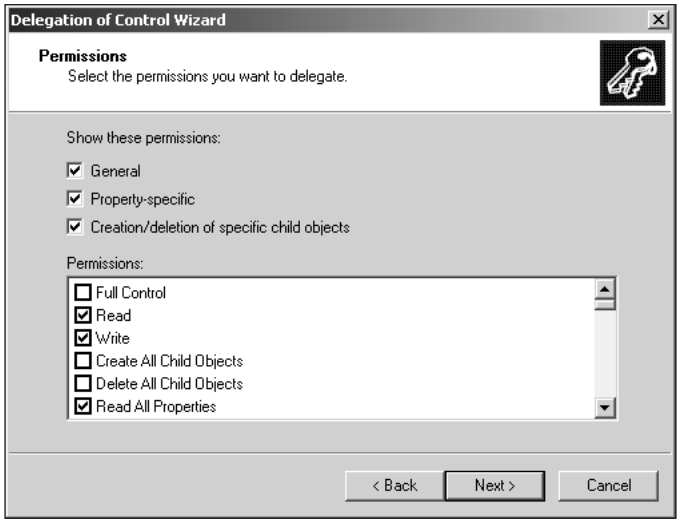

Figure 13-26 Within the Delegation of Control Wizard, you can choose the level of permissions you want the users or groups to have. Click on Next and then finish the wizard. At this point, the users and groups you selected will be able to add computer accounts to this OU

Prestaging Computers

If you do not wish to delegate control for users to add their own computers to an OU, you can use a process called **prestaging** to create computer accounts in advance and to ensure that each computer name is unique. Prestaging uses the computer's Globally Unique Identifier (GUID), which is stored in the BIOS of NetPC- or PC98-compatible computers, to identify the computer. The GUID is then stored with the computer account in Active Directory, ensuring that the specific computer that has the correct GUID will be the only computer to use the computer account. This is an excellent security measure. For example, suppose you know the username and password for a user who—as a potential RIS client—is authorized to add computers to a domain. You can run the Client Installation Wizard and access the RIS server, and you can even set up a domain computer, where you can start accessing network resources easily. It doesn't matter who you are, or what machine you're configuring; it can be a system you've brought from home, or you could be someone from the outside who really shouldn't be accessing the network but just got your very own domain computer through RIS. With prestaging, an administrator doesn't have to grant computer account creation rights to users.

In addition, by tying the computer's GUID to the computer account, an administrator can ensure that someone doesn't "borrow" a valid computer account for his or her own use. That way, you know that a specific computer is using a specific computer account at all times, reducing a potential security risk.

Chapter Summary

In this chapter, you learned about Windows 2000 Server's Remote Installation Services, an optional utility that allows a compatible RIS client computer to connect to an RIS server and install the Windows 2000 Professional OS. Some of the key topics included the following:

- RIS can install only Windows 2000 Professional. It cannot be used to install Windows 2000 Server, Windows NT, or Windows 9*x*.
- RIS is dependent on Active Directory, Group Policy, DNS, and DHCP.
- An RIS client must support the Preboot Execution Environment (PXE) either through the system BIOS or the network adapter.
- A select number of network adapters are supported by the RIS boot disk, which is used to emulate a PXE environment.
- RISetup.exe is used to create CD-based installation images.
- RIPrep.exe is used to create custom images that can contain Windows 2000 Professional as well as third-party applications.
- RIS servers must be authorized through DHCP before they can respond to client requests.

- An administrator can prestage computers for increased security.
- If computer accounts are not prestaged, a user must have computer object creation permissions to complete Windows 2000 Professional setup successfully.
- An administrator can use Group Policy to determine which client installation options will be available to the user.
- RIPrep cannot be used to image a computer with multiple hard-disk partitions.
- The Windows 2000 Professional installation directory must be on the boot partition for RIPrep to succeed.
- The image process erases all information currently on the RIS client computer's hard disk.